POLITECHNIKA GDAŃSKA

Karta przedmiotu

Nazwa i kod przedmiotu	Zarzadzanie bezpieczenstwem informacji, PG_00048285		
Kierunek studiów	Informatyka		
Data rozpoczęcia studiów	luty 2023 r.	Rok akademicki realizacji przedmiotu	2023/2024
Poziom kształcenia	II stopnia	Grupa zajęć	Grupa zajęć fakultatywnych Grupa zajęć powiązanych z prowadzonymi badaniami naukowymi w dziedzinie nauki związanej z kierunkiem - profil ogólnoakademicki
Forma studiów	stacjonarne	Sposób realizacji	na uczelni
Rok studiów	2	Język wykładowy	polski
Semestr studiów	3	Liczba punktów ECTS	3.0
Profil kształcenia	ogólnoakademicki	Forma zaliczenia	zaliczenie
Jednostka prowadząca	Wydział Elektroniki, Telekomunikacji i Informatyki -> Katedra Inżynierii Oprogramowania		
Imię i nazwisko wykładowcy (wykładowców)	Odpowiedzialny za przedmiot	dr hab. inż. Rafał Leszczyna	
	Prowadzący zajęcia z przedmiotu	dr hab. inż. Rafał Leszczyna dr inż. Andrzej Wardziński	

Formy zajęć i metody nauczania	Forma zajęć	Wykład	Ćwiczenia	Laboratorium	Projekt	Seminarium	RAZEM
	Liczba godzin zajęć	15.0	0.0	0.0	15.0	0.0	30
	W tym liczba godzin zajęć na odległość: 0.0						

Aktywność studenta i liczba godzin pracy	Aktywność studenta	Udział w zajęciach dydaktycznych, objętych planem studiów	Udział w konsultacjach	Praca własna studenta	RAZEM
	Liczba godzin pracy studenta	30	6.0	39.0	75

Cel przedmiotu	**Celem przedmiotu jest zrozumienie oraz pozyskanie przez studenta wiedzy na temat zarządzania bezpieczeństwem i prywatnością informacji z perspektywy analityka wymagań względem systemów informatycznych**

Efekty uczenia się przedmiotu

Efekt kierunkowy	Efekt z przedmiotu	Sposób weryfikacji i oceny efektu
[K7_W43] zna i rozumie w pogłębionym stopniu formalne, techniczne i społeczne aspekty działania złożonych systemów informatycznych w społeczeństwie informacyjnym i w globalnej infrastrukturze informacyjnej	Student rozumie istotę zagrożeń dotyczących bezpieczeństwa oraz prywatności, rozumie wzajemne relacje pomiędzy bezpieczeństwem i zaufaniem, pomiędzy użytecznością i bezpieczeństwem oraz rozumie wzajemne zależności pomiędzy pojęciami safety, security i privacy	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW2] Ocena wiedzy zawartej w prezentacji
[K7_W41] zna i rozumie w pogłębionym stopniu standardy, metody wytwarzania, cykl życia i trendy rozwojowe oprogramowania oraz systemów i aplikacji informacyjnych	Student rozumie pojęcie cyklu życia bezpieczeństwa oraz potrzebę procesowego podejścia do zapewniania bezpieczeństwa. Posiada również wiedzę na temat celów i zakresu głównych standardów dotyczących bezpieczeństwa informacji, w szczególności standardów serii ISO 27000 oraz IEC 62443	[SW3] Ocena wiedzy zawartej w opracowaniu tekstowym i projektowym [SW2] Ocena wiedzy zawartej w prezentacji
[K7_U02] potrafi wykonywać zadania związane z kierunkiem studiów oraz formułować i rozwiązywać problemy z wykorzystaniem nowej wiedzy z fizyki i innych dziedzin nauki	Student rozumie podstawowe pojęcia związane z analizą ryzyka dotyczącego bezpieczeństwa informacji oraz ochrony pred zagrożeniami bezpieczeństwa i potrafi posłużyć się tymi pojęciami analizując konkretny system IT	[SU5] Ocena umiejętności zaprezentowania wyników realizacji zadania [SU4] Ocena umiejętności korzystania z metod i narzędzi [SU2] Ocena umiejętności analizy informacji

Treści przedmiotu	1. Zasoby informacyjne I ich znaczenie; 2. Pojęcie i zakres bezpieczeństwa informacji; 3. Bezpieczeństwo a zaufanie; 4. Bezpieczeństwo a użyteczność; 5. Klasyfikacja i etykietowanie zasobów informacyjnych; 6. Ocena zagrożeń i podatności; 7. Ocena ryzyka dotyczącego zasobów informacyjnych; 8. Dobór zabezpieczeń – system zarządzania bezpieczeństwem informacji; 9. Wybrane techniki analizy ryzyka – drzewa ataków; 10. Standard ISO/IEC 27001:2013 – zakres, wymagania, ocena zgodności; 11. Prywatność (pojęcie, zakres, regulacje) oraz wybrane techniki zapewniania prywatności; 12. Relacje między pojęciami bezpieczeństwa (safety), zabezpieczenia (security) i prywatności (privacy); 13. Bezpieczne wytwarzanie oprogramowania 14. Zagrożenia bezpieczeństwa systemów SCADA (Supervisory Control And Data Acquisition).		
Wymagania wstępne i dodatkowe	Wcześniejsze uczestnictwo w przedmiocie *Inżynieria wymagań*		
Sposoby i kryteria oceniania osiąganych efektów uczenia się	Sposób oceniania (składowe)	Próg zaliczeniowy	Składowa oceny końcowej
	Projekt	45.0%	45.0%
	Egzamin pisemny	45.0%	45.0%
	Aktywność/obecność	10.0%	10.0%
Zalecana lista lektur	Podstawowa lista lektur	1. Standard ISO/IEC 27001(http://minf.vub.ac.be/marc/medinf/iso-27001-2013.pdf) 2. Standardy IEC/ISA 62443 (http://isa99.isa.org/ISA99%20Wiki/WP_List.aspx 3. Ross Anderson, Security Engineering, 2-nd edition, Wiley 2008 (online: http://www.cl.cam.ac.uk/~rja14/book.html)	
	Uzupełniająca lista lektur	1. Standard NIST SP 800-53 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)	
	Adresy eZasobów	Adresy na platformie eNauczanie: Zarządzanie bezpieczeństwem informacji - specjalność ISI -2024 - Moodle ID: 35301 https://enauczanie.pg.edu.pl/moodle/course/view.php?id=35301	
Przykładowe zagadnienia/ przykładowe pytania/ realizowane zadania			
Praktyki zawodowe w ramach przedmiotu	Nie dotyczy		